REMARKS

Claims 1-4, 7-8, 10, 13-16, 19-20, 22-30, 33-34, 37, and 39 are pending. Claims 1, 15, 25, and 33 are independent claims.

Reconsideration and allowance of the above-referenced application are respectfully requested.

Claim amendments are presented herein to obviate the current rejection. No new matter has been added.

35 USC § 102 / § 103

Claim 1-10, 13-22, 24-30 and 33-39 stand rejected under 35 USC 102(a) as allegedly being anticipated by Iyer. Claim 23 stands rejected under 35 USC § 103(a) as allegedly being unpatentable over Iyer in view of Tal. These rejections are respectfully traversed.

Claim 1 recites searching an entry associated with a network component in an aggregated data set to identify one or more pointers to a deployment policy tree and a pointer to a configuration tree, based on the identified one or more pointers to the deployment policy tree, searching the deployment policy tree to identify one or more policies directly associated with the network component and to identify one or more policies directly associated with the group, based on the identified pointer to the network configuration tree, searching the configuration tree to identify a parent node corresponding to a group to which the network component belongs to generate a list of one or more groups to which the network component belongs. Claims 15 and 33 contain similar features.

Claim 25 recites a policy based network management (PBNM) system that comprises a network configuration tree, a deployed policy tree, an aggregated data set, and one or more software components configured to identify one or more policies

associated with a network component, generate a list of one or more groups to which the network component belongs, and identify one or more policies associated with each of the groups in the generated list.

With the arrangement defined by claim 25, the aggregated data set includes one or more identity elements, one or more pointers to the deployed policy tree, and one or more pointers to the network configuration tree. Each identity element identifies a network component and has an associated network configuration tree pointer and one or more associated deployed policy tree pointers.

Iyer describes an arrangement in which a unified policy management system for an organization includes a central policy server so that policy information may be specified and distributed to remotely situated policy enforcers (see, inter alia, Iyer abstract). A central database and policy enforcer databases store policy settings that are configured as Lightweight Directory Access Protocol (LDAP) databases having a hierarchical object structure.

With Iyer a structure of entries in an LDAP database includes policy server domain objects, policy domain objects that have resource root objects and group root objects, devices, users, times, as well as groupings (see, inter alia, Iyer page 8, lines 16-31 and Fig. 2). However, the organization of such relationships is unclear and is contradicted by the specification of Iyer. For example, resource objects devices 204, users 206, hosts 208, services 210 are described as being organized in groups 212, 214, 216, and 218.

In contrast, the deployment policy tree and the network configuration tree recited in claim 1 provides a logical hierarchical framework in which one or more policies directly associated with the network component as well as one or more

policies directly associated with the group may be determined. Moreover, the configuration tree may be searched to identify a parent node corresponding to a group to which the network component belongs to generate a list of one or more groups to which the network component belongs. Iyer does not disclose such a hierarchical arrangement to generate a list of groups for a network node. Rather, Iyer is directed to the distribution of policies to a large number of policy enforcers as opposed to the determination of policies for a particular policy enforcer.

In addition, Iyer also fails to disclose an aggregated data set that includes an entry associated with the network component, with such entry identifying pointers to the deployment policy tree and the configuration tree that reduces or an aggregated data set that includes one or more identity elements that identify a network component and has an associated network configuration tree pointer and one or more associated deployed policy tree pointers.

Accordingly, claims 1, 15, 25 33, and their respective dependent claims are allowable.

Concluding Comments

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any

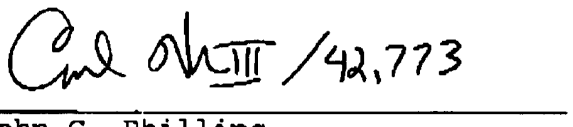
claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Kindly change the Attorney Docket Number for this matter to: 10559/503001/P11795.

Applicant asks that all claims be allowed. Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 7/20/05



John C. Phillips
Reg. No. 35,322
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer Number: **20985**
12390 El Camino Real
San Diego, CA 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10517414.doc